University of St. Thomas Journal of Law and Public Policy

Volume 11 | Issue 1 Article 4

The Internet of Things: Privacy Issues in a Connected World; Remarks Given at Protecting Virtual You: Individual and Informational Privacy in the Age of Big Data

Richard M. Martinez

THE INTERNET OF THINGS: PRIVACY ISSUES IN A CONNECTED WORLD REMARKS GIVEN AT PROTECTING VIRTUAL YOU: INDIVIDUAL AND INFORMATIONAL PRIVACY IN THE AGE OF BIG DATA

BY RICHARD M. MARTINEZ[1]

I'm going to be talking to you about the Internet of things today and I have sort of a painful appreciation of the fact that I am the only thing that's standing in between you and lunch as the last speaker, so I will try to keep things going at a quick pace just to make sure people don't start to look grumpy at me. Just to begin, just to kind of get on the same page, let me sort of lay out a practical definition of the Internet of things, and I'll start by saying, by asking really, how many of you have an Apple watch by chance today, that you're wearing? Ok, just two of us, and I just wore it for this event. Any Fitbits in the room? A few Fitbits. Ok, well you're already wired and connected and participating in the Internet of things.

The term is really a catch-all for devices that are connected. I sort of use the contrast between, we can dial back to earlier days of the web growing, the Internet developing and becoming a consumer platform. We measured people online, we measured human beings being connected to the Internet through their laptops, their desktops, more recently, smartphones and the like. And so, there was this constant benchmarking of how many more people and households were connected to the internet every year. In contrast today, what we have found is that we've had gizmos, things, gadgets, machines that are programed and running software on them, like your phone, like lightbulbs in your homes now, that are all interconnected, and we've now reached the point, in fact we did several years ago, where the number of devices, gizmos, things, IOT devices that are connected to the Internet far exceed the number of people that are connected to the Internet. And So we have these everyday examples of watches and Fitbits,

---

[1] Partner, Chair Data Privacy and Cybersecurity Group at Robins Kaplan. These remarks were given at the September 2016 symposium, "Protecting Virtual You: Individual and Informational Privacy in the Age of Big Data ," at the University of St. Thomas School of Law.

network cameras, so-called nanny cams that you might use in your home and check in on your kids while you're at work. Make sure your childcare provider is taking care of your kids, or they even have them for specialized interest. Every novelty interest you can think of. If you really love pets, you can watch your pet. And all these kind of things. We have Nest thermostats now and Honeywell has come along and done the same thing, where you can, your thermostat, something that never used to be connected, right? It was a great sensor, it took temperature readings, maybe humidity and the like, but that was about it. Now it's connected to the Internet. You can track your usage. You can phone home and have your house, or you can program your home from a distance to turn on earlier if you're coming home earlier and that kind of stuff. You have smart-meters that can gauge your water use and your electricity use without somebody having to physically come to your house and take those readings. You have in-store tracking. So-called beacons, which we'll talk about a little later, whereby use of different techniques. One being the presence of your smartphone on you. Retailers can track your presence in their store and your movement throughout their stores.

Specific advertising can be offered to you based on where you are. If any of you have, we might as well have a show of hands since there was only one iWatch user in here. How many of you have iPhones in here? How many of you are geeks like me, early adopters, and have already updated to the latest IOS. Great. So you already are using location-based services that track your presence, and maybe you've already picked up on this, will show you relevant applications when you're in a different place. So you might go to the gym and have health-related apps, exercise apps, pop up on your screen as the app that you might find helpful, that you might want to use. And again Fitbits and Apple watches are good examples. So, while the examples that I've started with are all in the consumer space, and they're probably ones that most of you have already had, at least in passing and perhaps some extensive contact and interaction with, there's also, on the consumer side of things, you can sort of broadly fit the categories of IOT devices as consumer and industrial. Now, on the consumer side, you have the phones that we've talked about, smart TVs which now have the ability to listen for your voice and hear you say play MSNBC, or depending on your preferences, play FOX News. And, voila, they will change the channel for you. They're also, of course, listening to you and sending your voice and sounds within your home, potentially, to some cloud service elsewhere.

You now have appliances. Everything from the washing machine that can send your app an indicator that the laundry is done, and it's time to switch it over to the dryer. No more excuses for whoever's job that is in the house. Same thing with kitchen appliances. People laugh about, or at least I laugh about, the example of your toaster talking to your oven. I can never figure

out why those two would need to talk to each other. But there are all sorts of sensors that will now say ok your oven is preheated for this or that, and the like. There is an ever-growing list of consumer-side applications, and also I would sort of lump onto that, medical devices that are going in that direction. Everything from, of course, pacemakers and infusion pumps the kind of things that you, when you go to a hospital and you get an IV, they'll regulate your intake of different medications, which now somebody decided would be a great idea to put WIFI and Bluetooth into, with all sorts of risks attended to that, to scales that have WIFI and Bluetooth, so when you weigh yourself in the morning, if you thought forgetting what your weight was one of the options, you can have your app track it and remind you of it. And better yet, you can have these other applications like glucose monitors and your Fitbits, all of these apps, in turn, can start collecting more and more data and sharing them with each other. That's one of the things that I'll talk about today is that sort of. The mental image I have is sort of the Russian nesting doll of interconnected applications and devices sharing information that are tracked about you, typically for some useful purpose. So you might be able to track your weight-gain while on a certain medication, or you can track different variables of your health, such as your physical activity and your blood pressure and your weight and have those things that you can use either for your own wellness or to help, for instance, your physician guide your care.

On the industrial side there is a whole other word of devices that are out there that are on factory floors that are tracking all sorts of processes that occur within the factory, the movement of inventory, of people. The whole electrical grid is now more and more connected by devices that allow us to control and optimize the grid, but of course necessarily make it that much more vulnerable. There's a whole smart cities movement afoot where cities are becoming controlled by devices. So everything from the lights that you see down the street to cameras that go to police departments to all sorts of infrastructure that's being changed. So, you know, of course we in the Twin Cities had the I-35W bridge collapse. You now have the ability to have smart bridges and smart structures where the concrete has sensors in it that can determine temperature, that can determine motion and movement, with the idea that you can detect before a failure ever occurs. You can detect weaknesses that are occurring and the like.

And we'll also see going forward as you start to see the intersection between demographic shifts that are coming and technology. We have a growing Asian population. There are more and more companies looking at how to use interconnected devices to help people as they grow older, to help family members. I have clients that—I can talk about some of this because it's public—that are working on projects that will allow you to watch mom and dad as they grow older at home. The idea of letting them

stay at home longer and they can start to detect certain things. So if Dad gets up every morning at 6:00, he lets the dog out, he gets the coffee, by using a simple video camera in the kitchen that can detect certain motions, you can allow kids across the country to check in and make sure somebody is OK at home. So you're going to see more and more of those applications. And one measure of the growth that is occurring in the Internet of things, but also a measure of the risks for privacy is that there are now search engines just for the Internet of things.

So consider it a Google or a Bing, if that's still a thing, for IOT devices. There are two of them that are pretty well known and popular. One is called Shodan and the other is called Thingful. And you can literally go on the Internet, type in the URL for these sites, and use them to find devices all over the world that are connected. It could be everything as mundane as a weather station sensor in your neighborhood to video cameras, nanny cameras, cameras that are in dormitories, that are in hospitals, that are in work places. And this is not only an indication of how much growth there is in IOT devices, but also shows you how easy it is to find devices that you bring into your home. And there are countless examples of people that have been able to go on and find home security cameras, nanny cameras, and the like that are on right now recording everything that is going on at home. And not through hacking of the devices, sadly, a lot of these devices are not protected in the manner that we would expect—at the highest level of security. So they might come with a default user names and passwords that are something like admin and password as the account name and the password. And you can find those devices easily and you can use these default passwords to enter them. In fact there have been cases of this and the FTC has already, as Professor Brown indicated, the FTC is sort of the de facto regulator in this space. They've brought cases, including notably one against TRENDnet, a well known maker of camera devices, for not having suitable security in their devices and making it all too easy to find private stuff going on at home.[2] In fact there were instance of not just spying on people, but there were people that were maliciously kind of dialing in. Some of these cameras have microphones and speakers, so you can say something to your kid, is the ideal case, but there were people actually yelling obscenities at children in the room through these cameras.
So, as I mentioned, these video cameras are certainly one of the more popular and ubiquitous examples of this, and there have been a number of FTC actions where they have gone after these companies for basically having very lax security. And having devices that can talk to each other. And this is an example with this Fox Cam camera, where they're able to tell

---

[2] "Decision and Order," *In the Matter of TRENDNET Inc.*, Docket No. C-4426 (January 16, 2014).

the camera was allowing other devices on the network to ping the camera and start talking to each other. So you can literally face a situation where you can envision a home, and the same thing can be applicable in the work place, but in a home when you start to add more and more layers of connected devices, your thermostat, your lightbulbs, and the like, where a security breach on any one of those might open the door to other devices. So think of the implication from a consumer standpoint and from the security and privacy standpoint. When you consider those click-through terms that you might be reviewing, if you do review them, for Product A, if Product A is talking to Product B, and you think you're OK with the privacy that Product A has established, you might have opened the door to some other product downstream to allow your private information to be accessed in turn.

And there are countless other examples that we can point to where all sorts of data, everything from your physical activity on a Fitbit, for example, the temperature in your home and the like, to now. I mentioned the family scale can have a WIFI connection to it. Withings is a company that is developing a lot of these kind of connected products, the family connected scale being another one of their products. They have this new thermo-scanning thermometer that not only takes a very accurate and quick reading of your body temperatures with a temporal scan, but it's tied to an app on your smartphone, which is a common way for a lot of these IOT devices to work. They have either some sort of connection to a hub in the home like an Amazon Alexa or to your smartphone. And so this will take readings, and you can imagine this is a kind of handy. If your child is sick, or you yourself are sick, and you want to track is my temperature going up or down during the course of the day and you can keep these things, but you can envision as well, from a collection of data standpoint, that there are other potential implications for all of these things that may not be apparent when you first decide whether you want to buy one of these things, as a consumer, and whether you want to sign on to whatever the privacy terms are. So for instance, something as seemingly innocuous as your body temperatures could easily be used to determine your general health, potentially could be used for insurance purposes. You could see it coming up in litigation for all sorts of reasons. Were you really sick? If you're somebody who has been out sick for an extended period of time and it turns out you don't have a temperature. You can see these many, many uses where the collection of data can become exploited or misused, or shall we say be used in a way you didn't originally contemplate.

And in the medical device space, I'll just sort of mention quickly, not only do you have the FTC regulating here, but you have the FDA asserting its authority as well, and they have—I won't go into much detail on this, just other than to mention--they're wading into this space. They're

trying, for the time being, to take a light touch approach in order to encourage development. So for the time being they've indicated they're not going to actively regulate things that fall within this sort of general wellness space as opposed to things that are actually a part of diagnosis or treatment. So for the time being, that's how that's working. They have also, the FDA itself, has also sort of started to get into the cyber security end of things, which of course has an implication on privacy, but they're just at the guidance standpoint for the time being.

And I won't mention—I won't go into the smart refrigerator for very long, but yet another one of these examples where now you've got the refrigerator that has a screen on it and talks to an app and keeps track of your food inside of it and tells you what you need to replenish, that kind of stuff. Again you can kind of see where something like this, which, frankly to many of us may seem like a pointless novelty, but who knows, someday this may become how all of our fridges look, and it's collecting stuff that's supposed to be helpful, but you can also see that, well, it can track how you eat, what you eat, how healthy, how much you eat, what you drink. And there's, of course, the possible misuse, you know, hackers, people getting into information that perhaps some of us wouldn't care if anybody wants to know what's in our fridge but other people would for other reasons.

And one other implication from a privacy standpoint that may not as apparent as you get more and more gadgets that are connected is the fact that there's a greater number of products that you now have to watch the security of. So for those of you who have iPads and iPhones, how many of you are on top of it anytime there's a new patch or security update, do you get to it right away? Imagine. We're now in a world where lightbulbs in your house require firmware updates. And as you get more and more devices like this that need tending to, that you're going to have to monitor, that have interconnectedness between them, you're going to see more and more risk and exposure. And to that end, literally this morning's Wall Street Journal has a story in the B Section the headline is "Hackers Hijack Video Cameras."[3] Attackers took control of some Chinese-made devices connected to the Internet. And basically there was a story last week, Brian Cribbs, the pretty well known security reporter. He was the guy who first came to fame, to attention, by having broken the story of the Target credit card breach, ironically enough, his website was shut down for a period of time last week through a denial of service attack, where you start to have lots and lots of computers, traditionally, start to all simultaneously access the site, and of course there's too much demand, and the site can be brought down. Well this was the first where they weren't using computers. They

---

[3] Drew Fitzgerald, "Hackers Infect Army of Cameras, DVRs For Massive Internet Attacks," THE WALL STREET JOURNAL, September 30, 2016.

created essentially a bot of devices, in this case security cameras and DVRs, and got all of those to simultaneously descend on Brian Cribbs' website. And you can see the same thing happening to you know shut down liberal newspapers during an election cycle, and you can go on and on. And it shows you the risk that is present in these IOT devices, and again, tying it to the idea of updating the, patching the software on my fridge. Probably something that's not likely. And even more far-fetched when you're talking about devices, this is a bad example because this at least has a screen, and it might actually be a little bit easier, you can image all the little gizmos in the home that don't have screens and the steps it would take to update them and keep them patched. So, some real risks that are underscored there.

So, bringing all this together, you can start to see that from a privacy standpoint, there are implications for how information is collected, what is going to be done with it, and all of the implications that come from having devices that start to talk to each other, sort of open the door for potential misuse. And when you have instances of information that you might think one device maker should access that you probably may not want others to access, or which create the opening within your home of releasing information you don't want to have collected, and all of these things have the possibility for defeating consumer expectations as you start to bring in more devices into your home. Have any of you purchased an Amazon Alexa by chance? OK, there's one early adopter in the back. You've no doubt saw the Super Bowl commercials about them. This is the device in your home that you talk to, that you can ask information of and the weather, but you can also use to control all the other devices in your home, so you can tell it to lower the temperature on your nest, you can tell it to turn on lightbulbs elsewhere in the house, or to dim shades, bring shades down, and the like. So this is the perfect example of the interconnectedness of devices and how you may have bought the lightbulbs from GE or Phillips and you may have bought the nest from Google, but suddenly to be able to access those things through an access point such as Amazon Alexa, you're not only on the front end agreeing to the terms of use and the privacy policies of the individual IOT devices that you have, but the gatekeeping device, the Alexa in this case, is going to regulate things as well.

There's a few slides on my set, that I'm not going to go through, that get into some of the regulatory landscape as well as some of the laws, sort of the legal and regulatory landscape that applies to the IOT. I'm just mentioning that because I'm not going to talk about them, but if you're interested in that, they are in the slides. My kind of quick takeaway on that, or the point to leave you with is that you have laws that clearly were not designed for the Internet of things, and that is the current legal landscape that we live in. You have laws, everything from state breach of notification

laws, and the Consumer Fraud and Abuse Act,[4] the Wiretap Act.[5] Now, the Wiretap Act was last amended in 1986, and it brought into effect the Stored Communications Act[6] and, broadly, this legislation called ECPA. All acts that can apply to the IOT and are impacting, certainly when you start talking about cloud sharing of information. But my key takeaway for you from a privacy standpoint, is that the laws that are there to regulate the space right now predate the internet in many cases, and certainly have not been updated any time recently.

So, the FTC has indicated that they're going to be monitoring this space. They've had a symposium earlier last year, and they started back in 2013 to really have some sessions on it, focused on it. They're still at the early stages, as I mentioned, there have been some instances of enforcement throughout. One example that I want to kind of use to illustrate a point is the photo on the left. One of the many devices that are coming online now, IOT devices, are so-called smart garage door openers. Chamberlain, which is a fairly common brand of garage door openers has one of these apps, very easy to kind of retro fit, you put this device in your garage, you give it access to your WIFI, and then, through a remote app you can send a signal to open your door, for example to let a repair person come in, to let someone who's locked out in, that kind of thing. Not to try to make something simple deep, but here's the point I want to drive home with this device, and that is that with the Internet of things, you're starting to get an amazing amount of collection of data, so you have something here that is essentially never was recorded data in the past. For as long as there has been an electric garage door opener, you might have an opener in your car, you might have one of those keypads outside your door, but there has never been anything or anyone who has been interested in tracking how many times a day your garage door opens, when it opens, and when it closes. It just wasn't a thing. As these devices come online, of course they're connected to the cloud, and they can send you messages or emails alerting you to the fact that your door has been opened to make sure you close the door and that kind of stuff. But think of this for a moment. You now have this treasure trove of data—garage door opening—that never was collected before. And you can play this out in your mind as a thought exercise of all the types of data that can be collected today and going forward that may have some potential value to someone. You may be asking yourself, who cares? Well, it lets you figure out what time you get leave for work, what time you get home, when your kids leave for school, when your kids get home, and by extension, when your kids are alone. There are all sorts of reasons why this data might be something you do or don't want shared, and

---

[4] 18 U.S.C. § 1030.
[5] 18 U.S.C. § 2511.
[6] 18 U.S.C ch. 121 § 2701-2712

as we go forward in time, you start to overlay the impact of artificial intelligence on this. You have more and more data sets that are collected, and you have people who are starting to find the interconnectedness on data, the interrelationships between data. Right, so garage door openings, coupled by city, by state, by other factors, and before you know it, a mundane kind of piece of data that you wouldn't even worry about—your garage door opening—can become much more valuable to things, I certainly can't dream of it now, but no doubt will come forward.

And so the implication from a privacy standpoint is that when you're making these privacy determinations as a consumer, you may be agreeing to terms today that might not make sense five years later. As that data has some other, either commercial application, or some other use that may not fit with your privacy considerations. And so that's an important factor both for consumers today, for viewing privacy issues today, and also for policy makers to consider going forward as you look at the ability to adjust policy terms, and the same thing applies when you have changes in ownership of data. So as this has happened many times, many of you have probably seen very recently, just to use a headline as an example, Facebook bought WhatsApp, the messaging service.[7] When WhatsApp was started, it was a messaging services with a very strict view on privacy. We wouldn't share any of your information on who you're communicating with and who you're messaging with. Facebook bought it, paid a lot of money for it, and not saying this critically, but they obviously paid money for a reason, and they're now changing the policy terms, and the same thing plays out when data owned by one company who you bought something from gets sold to somebody else, and seeing these things play out is an interesting thing. So that, I think I'll close my remarks and open it up to questions.

---

[7] Dan Tynan, "WhatsApp Privacy Backlash: Facebook Angers Users by Harvesting their Data," THE GUARDIAN, August 25, 2016.